APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,448	04/27/2001	Gregory Neil Houston	05456.105005	9082

69151   7590   06/28/2007

KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA, GA 30309-3521

EXAMINER
PICH, PONNOREAY

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/28/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
09844448	4/27/2001	HOUSTON ET AL.	05456.105005

KING & SPALDING, LLP
INTELLECTUAL PROPERTY DEPT. - PATENTS
1180 PEACHTREE STREET, N.E.
ATLANTA, GA 30309-3521

EXAMINER
Ponnoreay Pich

ART UNIT	PAPER
2135	20070623

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

This communication letter is sent in response to the Appeal Center's request that section 9 of the Examiner's Answer include a concise explaination of the grounds of rejections. The attached is the revised Examiner's Answer with corrections as required by the Appeal Center. The deadline for appellant to respond to this letter is two months from the mailing date of this letter, see MPEP 1208.

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

MAILED

Application Number: 09/844,448
Filing Date: April 27, 2001
Appellant(s): HOUSTON ET AL.

JUN 2 7 2007

Technology Center 2100

Kelly L. Broome (Reg. # 54,004)
<u>For Appellant</u>

Revised
EXAMINER'S ANSWER

This is in response to the appeal brief filed 2/20/2007 appealing from the Office action

mailed 11/17/2006.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,088,804	Hill et al	6-2000
6,775,657	Baker	8-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 27-29, and 31-32 are rejected under 35 U.S.C. 102(e) as being

anticipated by Hill et al, US Patent No. 6088804, hereinafter "Hill" (Cited in PTO

892 01/22/03).

As per claim 27:

Hill discloses "A computer-implemented system for managing security event data

collected from a plurality of security devices (Fig 1) comprising:

a plurality of security devices operable for generating security event data (e.g.

simulated attack) comprising a plurality of alerts (e.g. security event types) that are

generated in response to detecting a security event in a distributed computing

environment; " in (Col 4 lines 53-55, and Col 5 lines 320-35 and lines 52-55);

> **Data about security events is collected by security agents 36 and**
> **transmitted via links 28, links 32, and a communication link 38 to a**
> **processor**
> **40**.
>
> **For purposes of this description, an attack is defined as a plurality of**
> **security events 50 occurring substantially concurrently in a given sampling**
> **period at a plurality of nodes 24 (FIG. 1). The sampling period is an**
> **arbitrary amount of time that is of a sufficient length to receive enough**
> **security events to form an attack**
> **signature (discussed below) for an attack.**
>
> A simulated attack includes at least one of security event types 56,
> but more realistically **a simulated attack constitutes several security event**
> **types 56 as illustrated in first simulated attack 55.**

"an event manager (SOM Processor 40) coupled to the security devices, the

even manager operable for collecting security event data from the security devices and

analyzing the security event data with scope criteria (signature) comprising <u>one or more</u>

definable variables operable for analyzing <u>and filtering</u> the security event data, <u>the</u>

<u>variables comprising **at least one** o</u>f a location of a security event , a source of security

event, a destination address of the security event, **a security event type**, a priority of a

security event, and an identification of a system that detected a security event," in (Col 5

line 39 to Col 6 line 20) <u>and</u>

> **<u>In this example, security event types 56 include destructive virus,
> snooping virus, worm, Trojan horse, FTP requests, and network overload.</u>**
>
> In addition to security event types 56 and percentage of security events
> 50 per event type in column 58, <u>training signatures 53 include location
> identifiers 60.</u> **<u>Location identifiers 60 identify the nodes 24 in network 22
> where security events may take place.</u>** Location identifiers 60 are important
> for ascertaining an attack severity 61 for each of simulated attacks 52.
> Attack severity 61 is a level of security breach that one of simulated attacks
> 52 could cause computer network 22. The greater attack severity 61, the more
> damaging the security breach would be.
>
> (34)   Following task 98, a task 100 is performed by **<u>SOM processor 40 (FIG. 1).
> SOM processor 40 compares a vector representative of first attack
> signature 94
> (FIG. 6) to each of training signatures 53</u>** as mapped in display map 66 (FIG.
> 4).

> <u>the event manager operable for applying the scope criteria to the security event</u>

<u>data to produce result data</u>" in (Col 8 lines 35-47)<u>; and</u>

> (35) **<u>In response to comparing task 100, a task 102 selects one of training</u>**

**signatures 53 that most closely matches attack signature. With reference back
to FIG. 3, the security event types 56 and frequency of security events 50
shown in column 58 of training signature 54 most closely resembles first attack
92. Those skilled in the art will recognize that other factors will contribute
to the selection of a most closely resembling training signature.** Other
factors may include but are not limited to, the location identifiers for each
of the affected nodes, network hierarchy, and so forth.

"one or more clients (Nodes 24) coupled to the event manager operable to

perform an action in response to receiving analyzed security event data from the event

manager and displaying the result data comprising filtered alerts based on the scope

criteria" in (Col 8 lines 4-11, and Col 8 line 63 to Col 9 line 7).

(30)   In response to task 82, a task 86 is performed through each of security
agents 36. **Task 86 causes SOM processor 40 to be notified of an outcome
of the
repulsing task through one of security agents 36 associated with that node
24.
The notification may include data describing a security event type, a
location
identifier for the node 24, and whether or not the attack was successfully
repulsed.** Following notification task 86, program control proceeds to a task
88.

As per claim 28:
Hill discloses "the system of claim 27, wherein the event manager comprises a

database server operable for storing the collected security event data and the analyzed

security event data" in (Col 8 lines 12-19, and Col 7 lines 45-65)/

As per claim 29:

Hill discloses the system of claim 27, wherein the event manager comprises an

application server operable for creating an incident from the security event data for

preparing a response (Col 8 lines 1-21).

As per claim 31:

Hill discloses the system of Claim 27, wherein multiple clients operable for receiving

analyzed security data are coupled to the event manager (Col 8 lines 1-21).

As per claim 32:

Hill discloses "The method of Claim 27, wherein the action performed by the client is

rendering a chart containing analyzed security event data (Figure 7).

Claim s 1-26, 30, and 33-59 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Hill et al, US Patent No. 6088804, hereinafter "Hill" (Cited in

PTO 892 01/22/03) in view of Baker, US/6775657.

As per claims 1, 18, 34, and 49:

Hill discloses "A method for managing security event data collected from a security

devices in a distributed computing environment" in (Figure 1) "comprising the steps of:

generating <u>security event data (e.g. attack) comprising</u> a plurality of alerts (e.g.

security event types) with a plurality of security devices at a first location (e.g. SOM

Processor 40) <u>in response to detecting a security event in a distributed computing</u>

<u>environment;</u>" in (Col 4 lines 53-55, and Col 5 lines 320-35 and lines 52-55);

> **Data about security events is collected by security agents 36 and**
> **transmitted via links 28, links 32, and a communication link 38 to a**
> **processor**
> **40.**

> **For purposes of this description, an attack is defined as a plurality of**
> **security events 50 occurring substantially concurrently in a given sampling**
> **period at a plurality of nodes 24 (FIG. 1). The sampling period is an**
> **arbitrary amount of time that is of a sufficient length to receive enough**
> **security events to form an attack**
> **signature (discussed below) for an attack.**

> **A simulated attack includes at least one of security event types 56,**
> **but more realistically a simulated attack constitutes several security event**
> **types 56 as illustrated in first simulated attack 55.**

"providing *one or more variables* operable for analyzing and filtering <u>the</u>

security event data, the variables *comprising at least one of* a location of a security

event, a source of security event, a destination address of the security event, <u>a security</u>

<u>event type</u>, a priority of a security event, and an identification of a system that detected

a security event" in (Col 5 line 39 to Col 6 line 20);

> **In this example, security event types 56 include destructive virus,**
> **snooping virus, worm, Trojan horse, FTP requests, and network overload.**

> In addition to security event types 56 and percentage of security events
> 50 per event type in column 58, <u>training signatures 53 include location</u>
> <u>identifiers 60.</u> **Location identifiers 60 identify the nodes 24 in network 22**
> **where security events may take place.** Location identifiers 60 are important
> for ascertaining an attack severity 61 for each of simulated attacks 52.
> Attack severity 61 is a level of security breach that one of simulated attacks
> 52 could cause computer network 22. The greater attack severity 61, the more
> damaging the security breach would be.

"creating scope criteria (e.g. Training Signature 53) by *selecting one or more*

(Hill teaches of training the scope criteria using the event type variable) of the variables

(security event types and node identification) operable for analyzing and filtering the

security event data (attack) " in (Col 5 lines 46-65, Col 5 line 65 to Col 6 line 5);

> **Training signatures 53 for simulated attacks 52 are defined by a**
> **plurality of security events 50 of at least one security event type 56 in this**
> **example.** Security events 50 are presented in database 48 in a column 58 as a
> percentage of security events per event type. In other words, column 58
> represents the numbers of nodes 24 (FIG. 1) affected by each of security event
> types 56. A simulated attack includes at least one of security event types 56,
> but more realistically a simulated attack constitutes several security event
> types 56 as illustrated in first simulated attack 55. Each of security event
> types 56 are capable of causing an anti-security effect on computer network 22.
> In other words, the attacker is performing an unauthorized action on network
> 22. In this example, **security event types 56 include destructive virus,**
> **snooping virus, worm, Trojan horse, FTP requests, and network overload.**
> However, those skilled in the art will recognize that security event types may
> include these and/or additional evolving types of security events relative to
> the computer network for which dynamic network security system 20 (FIG. 1) is
> used.

> In addition to security event types 56 and percentage of security events
> 50 per event type in column 58, **training signatures 53 include location**
> **identifiers 60**. Location identifiers 60 identify the nodes 24 in network 22
> where security events may take place. Location identifiers 60 are important
> for ascertaining an attack severity 61 for each of simulated attacks 52.

"collecting security event data generated by the plurality of security devices

located at a first location" in (Col 4 lines 53-55);

> **Data about security events is collected by security agents 36 and**
> **transmitted via links 28, links 32, and a communication link 38 to a**
> **processor**
> **40**

> "*storing the collected security event data at a second location* "

"analyzing and filtering the collected security event data with the scope criteria to

produce result data" in (Col 8 lines 35-46);

(34) Following task 98, a task 100 is performed by S**OM processor 40 (FIG. 1).
**
**SOM processor 40 compares a vector representative of first attack
signature 94
(FIG. 6) to each of training signatures 53** as mapped in display map 66 (FIG.
.4).

(35) **In response to comparing task 100, a task 102 selects one of training
signatures 53 that most closely matches attack signature. With reference
back
to FIG. 3, the security event types 56 and frequency of security events 50
shown in column 58 of training signature 54 most closely resembles first
attack
92. Those skilled in the art will recognize that other factors will contribute
to the selection of a most closely resembling training signature.** Other
factors may include but are not limited to, the location identifiers for each
of the affected nodes, network hierarchy, and so forth.

"transmitting the result data to one or more clients; and

displaying the result data comprising filtered alerts based on the scope criteria" in

(Col 8 lines 4-11, and Col 8 line 63 to Col 9 line 7).

(30) In response to task 82, a task 86 is performed through each of security
agents 36. **Task 86 causes SOM processor 40 to be notified of an outcome
of the
repulsing task through one of security agents 36 associated with that node
24.
The notification may include data describing a security event type, a
location
identifier for the node 24, and whether or not the attack was successfully
repulsed.** Following notification task 86, program control proceeds to a task
88.

However, Hill does directly teach "storing the collected security event data at a

second location". Hill does teach of a security events database in Col 7 lines 40-45.

Nevertheless, Baker teaches Multilayered Intrusion Detection System and

Method, which includes a method of collecting security event data and storing it in a

multiple security event database for availability purpose in (Col 8 lines 45-47).

Therefore, it would have been obvious at the time of the invention was made for

one having ordinary skill in the art to modify Hill's teaching to incorporate Baker's

disclosures of having security event database at different location in the network for

availability purpose (Col 8 lines 45-47).

As per claims 2, 21, 35, and 54:
Hill discloses "The method of claims 1, 16, 34, and 49, further comprising storing one or

more of the scope criteria, the security event data, and the result data in a database

(Col 8 lines 12-19).

As per claim 3, 5, 20, 30 and 36:
Hill discloses "the method of claims 1, 16, and 27, wherein the first location is a

distributed computing environment (Figure 1), the second location is a database server

(Baker, Col 8 lines 45-47), and the third location is an application server (Col 5 lines 15-

20) to which the plurality of clients are coupled".

As per claims 4, 14, 19, 38, 47, and 53:
Hill discloses "the method of claims 1, 16, 34, and 49, wherein collecting the

security event data comprises generating security event data from a sensor" in (Col 4

lines 30-40);

"sending the security event data from the sensor to a collector" in (Col 8 lines 12-

19); and

"converting the event data to a common format" in (Col 5 lines 37).

As per claims 6 and 39:

Hill discloses "the method of claims 1 and 35, further comprising searching the

stored security event data for additional information identifying a security event" in (Col

5 lines 26-45).

As per claims 7 and 40:

Hill discloses "the method of claims 1 and 35, further comprising: polling a

database server for current stored security event data;

analyzing the current stored security event data to produce current result data;

and

rendering the current result data" in (Col 5 lines 26-45).

As per claims 8 and 41:

Hill discloses "The method of claims 1 and 34, further comprising polling for messages

containing information about scope criteria, security event data, or result data (Col 5

lines 26-45).

As per claims 9 and 42:

Hill discloses "The method of claims 1 and 34, further comprising pushing messages to

a client wherein the messages contain information about scope criteria, security event

data, or result data (Col 4 lines 30-40, and Col 8 lines 4-11).

As per claims 10, 17, 43, and 50:

Hill discloses "The method of claims 1, 16, 34, and 49, wherein the step of rendering

result data comprises presenting the result data in a chart format (Figure 7).

As per claims 11, 22, 44, and 55:

Hill discloses "The method of claims 1, 16, and 34, wherein in response to analyzing the

collected security event data, an action is executed (Col 7 line 63 to Col 8 line 12).

As per claims 12, 23, 45, and 56:

Hill and Baker disclose "The method of claims 11, 22, and 44.

However, Hill does not mention the action is clearing security event data from

storage.

Nevertheless, it would have been obvious at the time of the invention for one

having ordinary skill in the art to realize that the capability of clearing out the data must

be exist in the invention of Hill, since it is inevitable to contain unlimited data in any

storage devices.

As per claims 13, 24, 46, and 57:

Hill discloses "The method of claims 11, 22, 44, and 55, wherein the action is creating

an incident from result data for preparing a response (Col 7 line 63 to Col 8 line 12).

As per claims 15, 26, 48, and 59:

Hill discloses "A computer-readable medium having computer-executable

instructions for performing the steps recited in claims 1, and 34" in (Col 35-45)

As per claim 16:

The rejection basis of claim 1 is incorporate. Further, Hill discloses applying the scope

criteria to the security event data at a third location to produce a result, the result

accessible by a plurality of clients coupled to a server" in (Fig 1, Col 8 lines 15-35, and

Col 5 lines 45-65).

As per claim 25:

Hill discloses "the method of claim 16, further comprising applying additional scope

criteria to a plurality of results" in (Col 7 lines 40-63).

As per claim 33:

Hill discloses "The method of Claim 1, further comprising the step of rendering the result

data in a manageable format for the plurality of clients (Figure 7).

As per claims 37, and 51-52:

Hill discloses "The method of Claims 34, and 49, further comprising the step of creating

and editing the scope criteria for filtering the security event data (Col 5 lines 1-6, and

Col.5 lines 25-38).

As per claim 58:

Hill discloses "the method of claim 49, further comprising applying additional scope

criteria to a plurality of results" in (Col 8 lines 35-47, and Col 9 lines 35-45).

(10) Response to Argument

Please note that to make it easier for the reader to follow along, the examiner will use the same headings as the appellant in traversing appellant's arguments.

<u>Rejection of claims as obvious over 35 USC 102(e)</u>

First the examiner notes that with respect to appellant's heading that the question of obviousness falls under 35 USC 103, while anticipation falls under 35 USC 102. Thus the examiner assumes the above heading used by appellant which refers to rejection of claims as "obvious" over 35 USC 102(e) as being an unintentional mistake.

<u>Independent Claim 27</u>

Appellant's arguments with respect to claim 27 begin on page 13 of appeal brief filed and continue to page 17. Appellant argues that Hill does not teach "an event manager that is operable for analyzing and filtering the security event data with scope criteria comprising one or more defined variables operable for analyzing and filtering the security event data" (see page 16 of appeal brief). Appellant argues that simply displaying attack status information as taught by Hill is not the same as "analyzing and filtering the security event data with scope criteria comprising one or more defined variables operable for analyzing and filtering the security event data". The examiner

respectfully disagrees. Even appellant's summary of what Hill teaches (pages 13-16 of

filed appeal brief) shows that this limitation is met by Hill. On page 14 of the appeal

brief, appellant states that Hill discloses a database of simulated attack information.

The simulated attack information/attack signatures can be considered "scope criteria

comprising one or more defined variables operable for analyzing and filtering security

event data" since it is used for comparison with network event data to determine if the

event data corresponds to any known attack types as well as used to determine the

severity of the attack. Note that as discussed in cited column 5, lines 46-50, the

signature of the attacks are defined by at least one security event, i.e. defined variables.

In the first two paragraphs on page 16 of the filed appeal brief, appellant summarizes

how Hill's system monitors and analyzes network traffic data, i.e. security event data,

comparing the network traffic data to the simulated attack signatures stored in a

database as seen in Figure 3 of Hill. This analysis is then used to form the network

display seen in Figure 7 of Hill. Display map 66 in Figure 7 shows the attacks, i.e.

security event data, having been sorted/filtered by severity (col 6, lines 53-60 of Hill)

and by attack type (col 6, lines 61-67 of Hill). Despite appellant's argument that simply

displaying attack status information is not the same as "analyzing and filtering the

security event data with scope criteria comprising one or more defined variables

operable for analyzing and filtering the security event data", the examiner respectfully

submits that unless the network event data, i.e. security event data, were analyzed and

filtered using the attack signatures, i.e. scope criteria, stored in database 48, the attacks

could not have been filtered by attack severity and attack type for display. The data is

also analyzed and filtered so that the security event type and location is also determined

as evidenced by table 108 in Figure 7.

In short, analyzing and filtering the security event data with scope criteria which

comprises one or more defined variables...reads on Hill's teachings of comparing the

network traffic data with the signature data stored in the database and displaying the

result of the analysis based on attack severity and type as seen in Figure 7. If analysis

and filtering of the network traffic data was not done, then Hill's invention could not have

displayed the attacks by severity, type, and location. The component of Hill's invention

that performed these processes can be considered an event manager.

Dependent Claims 28-33

Appellant's arguments for claims 28-33 are based on dependency on claim 27

and are traversed because the arguments for claim 7 are traversed.

Rejection of claims as obvious over 35 USC 103(a)

Independent claims 1, 16, 34, and 49

In the paragraph which spans pages 18-19 of the filed appeal brief, appellant

argues that Hill and Baker fails to teach: (1) providing one or more variables operable

for analyzing and filtering the security event data, the variables comprising at least one

of a location of a security event, a source of security even, a destination of the security

event, a security event type, a priority of a security event, and an identification of a

system that detected a security event"; (2) "creating scope criteria by selecting one or

more of the variables operable for analyzing and filtering the security event data"; and

(3) "analyzing and filtering the collected security event data with the scope criteria to

produce result data". The examiner respectfully disagrees—Hill does in fact teach all

three of these limitations.

As per the limitation of providing one or more variables operable for analyzing

and filtering the security event data, the variables comprising at least one of a location

of a security event, a source of security event, a destination of the security event, a

security event type, a priority of a security event, and an identification of a system that

detected a security event, it is met by Hill having the database of simulated attacks, i.e.

attack signatures (col 5, lines 21-37). The cited section shows that the simulated attack

is a defined by a plurality of security events, i.e. variables. Those variables comprise at

least the location of a security event, source of a security event, and a security event

type (col 5, line 45-col 6, line 8). As discussed in the traversal of claim 27, the variables

which makes up the attack signatures are used, i.e. operable, for analyzing and filtering

the security event data. Thus the limitation is met by Hill.

As per the limitation of creating scope criteria by selecting one or more of the

variables operable for analyzing and filtering the security event data, the sections cited

in the Final Office action (col 5, line 46-col 6, line 5) shows that the training

signatures/attack signatures for simulated attacks are comprised of security event types, i.e. variables, which includes at least the location of a security event, source of a security event, and a security event type. These variables are operable for analyzing and filtering the security event data. The claimed scope criteria read on the disclosed training signatures formed from one or more selected security event types and because they exist in Hill's invention, they were created. Thus, the limitation is met by Hill.

As per the limitation of analyzing and filtering the collected security event data with the scope criteria to produce result data, it was already discussed in the traversal of claim 27 how Hill taught analyzing and filtering the collected security event data with the scope criteria. The result of the analysis and filtering is the output display seen in Figure 7, i.e. result data that is produced.

It is noted that while appellant argues that the references do not teach the above limitations under contention, appellant did not argue whether or not the references are combinable to reject the claims as a whole under 35 USC 103. Appellant also did not argue the motivation given in the Final Office action for combining the two references. As such, it is assumed that appellant agrees that the references are combinable and that one of ordinary skill in the art of networking and network security would have been motivated to combine the teachings of Hill and Baker for the reason given in the Final Office action in the third paragraph on page 10, i.e. for availability purposes. Thus claims 1, 16, 34, and 49 were properly rejected under 35 USC 103 as being obvious over Hill and Baker since the combination of Hill and Baker renders obvious all the limitations recited in the claims and it was established that one of ordinary skill in the art

would have been motivated to combine the teachings of the prior art as recited in the

claims.

<u>Dependent Claims 2-15, 17-26, 35-48, and 50-59</u>

The arguments for these claims are based on dependency on claims 1, 16, 34,

and 49. Because the independent claims are not allowable, the dependent claims are
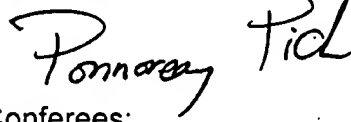
also not allowable.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the

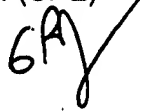Related Appeals and Interferences section of this examiner's answer.

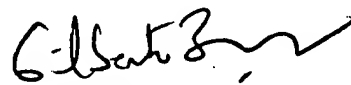For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Ponnoreay Pich

Conferees:

Gilberto Barron Jr. (SPE)

Benjamin Lanier

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100